IN THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF OKLAHOMA

1. LAURA DOUGHTY AND 2. AMANDA FISCHER, individually and on behalf of all similarly situated persons, Plaintiff, v. 1. CENTRALSQUARE TECHNOLOGIES, LLC and 2. CITY OF NORMAN, OKLAHOMA, a municipal corporation, Defendants.	Case No. 5:20-cv-00500-G Hon. Charles B. Goodwin **PLAINTIFFS' FIRST AMENDED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Laura Doughty and Amanda Fischer, on behalf of themselves and all similarly situated persons, bring this First Amended Class Action Complaint (the "Complaint") against Defendant CentralSquare Technologies, LLC ("CentralSquare") and City of Norman ("Norman"), based on personal knowledge and the investigation of counsel, and allege the following:

INTRODUCTION

1. This is an action to recover damages from CentralSquare for the harm suffered by Plaintiffs and a nationwide class of persons whose payment card information was stolen as a result of a data breach on CentralSquare's payment software, Click2Gov.

2. Click2Gov is a payment processing service provided by CentralSquare and used by municipalities across the United States to collect various payments, including utility bills, parking tickets, taxes, and similar payments.

3. Through this action, Plaintiff Doughty also seeks to obtain refunds for herself and all members of the Norman Subclass (defined below) for fees collected by Norman to provide for the security of their payment card transactions.

4. From 2017 to 2019, CentralSquare's customers, including Norman, experienced cybersecurity intrusions to CentralSquare's Click2Gov payment portal that compromised the payment card and related information, including names, card numbers, expiration dates, and security codes (collectively, "Payment Data") of at least 300,000 individuals.

5. Payment Data was later sold by the cybercriminals responsible for the cybersecurity intrusions to identity thieves on the dark web.[1] Victims, including Plaintiffs and members of the purported "Class" (defined below) they seek to represent, were residents of dozens of small-to-medium-sized municipalities across the United States.

6. Specifically, on October 13, 2017, Superion (now merged into CentralSquare) CEO, Simon Angove, released a statement acknowledging that its Click2Gov online utilities payment portal customers had experienced a data breach.

7. On November 7, 2019, Norman also reported that a data breach occurred on its Click2Gov online utilities payment portal.

8. Since mid-2017, hackers have been attracted to CentralSquare's Click2Gov payment portal. The first wave of cyber hacks against CentralSquare began in 2017 and

[1]Stas Alforov & Christopher Thomas, *Second Wave of Click2Gov Breaches Hits United States*, GEMINI ADVISORY (Sept. 19, 2019), https://geminiadvisory.io/second-wave-of-click2gov-breaches-hits-united-states/.

ended in 2018, followed by a second wave of cyber hacks that began in August 2019 and ended in October 2019. These two waves of cybersecurity intrusions against CentralSquare's Click2Gov payment portal will be collectively referred to herein as the "Data Breach."

9. As a direct result of the Data Breach, Plaintiffs and Class Members (defined below) suffered fraudulent charges, had their payment cards canceled, lost the use of their funds, lost time (i) contesting charges, (ii) trying to claw back funds stolen from their bank accounts, and (iii) driving to and from banks and credit unions, and some have even had to cancel accounts.

10. Plaintiffs bring this action individually and on behalf of Class Members to hold CentralSquare accountable for the harm they have suffered resulting from the Data Breach.

11. Plaintiff Doughty also brings this action individually and on behalf of the Norman Subclass in order to hold Norman accountable for charging its utility customers additional fees for payment card security that was never provided, and then subsequently failing to refund those fees.

PARTIES

12. Plaintiff Laura Doughty is, and at all relevant times to this action was, a citizen of Oklahoma and a resident of the City of Norman, Cleveland County, Oklahoma.

13. Plaintiff Amanda Fischer is, and at all relevant times to this action was, a citizen of Florida and a resident of the City of Margate, Broward County, Florida.

14. Defendant CentralSquare Technologies, LLC, is a Delaware limited liability company headquartered at 1000 Business Center Dr., Lake Mary, Florida 32746. Upon information and belief, CentralSquare is a citizen of Florida. CentralSquare is licensed to do business in Oklahoma as a foreign limited liability company and conducted business in Oklahoma at all relevant times to this action.

15. CentralSquare is a company whose mission is "[t]o create the broadest, smartest and most agile software platform for building safer, smarter communities."[2]

16. CentralSquare also represents itself as the go-to payment technology provider for public entities:

> "A central square is a place where citizens interact with their government, whether it be at city hall, police or fire station, or a hospital. "To square" is designed to communicate taking communities to the next level, and the four corners of a square refer to the four businesses that came together to form CentralSquare. CentralSquare emphasizes putting citizens at the center of everything we offer. We partner with more than 7,500 public sector agencies across North America, bringing together two primary drivers for improving people's lives—technology and government."[3]

[2] "About Us," CentralSquare Technologies, https://www.centralsquare.com/about-us, (last visit on April 14, 2020).
[3] *Id.*

17. Norman is an Oklahoma municipal corporation located in Cleveland County, Oklahoma.

JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. There are more than 100 putative class members, and at least some members of the proposed Class have a different citizenship from CentralSquare and Norman.

19. This Court has jurisdiction over CentralSquare and Norman and venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because both CentralSquare and Norman conduct their business in and through this District and Class Members residing in this District have suffered harm as a result of the Data Breach.

STATEMENT OF FACTS

A. The Data Breach

20. As early as the spring of 2017, numerous reports from local news outlets began to report on instances of payment card data breaches that were linked to local utility payment systems. As researchers and reporters focused in on this first wave of the Data Breach, one common denominator emerged: CentralSquare's Click2Gov payment software.[4]

[4]Stas Alforov, *Dozens of Municipalities Exposed in Click2Gov Software Compromise*, GEMINI ADVISORY (Dec. 18, 2018), https://geminiadvisory.io/hacked-click2gov-exposed-payment-data/.

21. In October 2017, Simon Angove, the CEO of Superion (later merged into CentralSquare) publicly acknowledged the growing number of data security incidents. He stated:

> "Recently we received reports of suspicious activity involving a small number of our customers' computer networks, including possible attempts to steal personally identifiable information … We have notified Superion customers about the suspicious activity and have continued to work closely with the small number of affected customers throughout our investigation. As part of our investigation we have identified and notified our customers of certain potential vulnerabilities in the security of their network and provided them with recommendations for addressing the same."[5]

22. This "small number of affected customers" began to increase.

23. As a result of the first wave of the Data Breach, the Payment Data of tens of thousands of individuals who made payments through the Click2Gov portal at dozens of cities was stolen, at least in part because of a failure to regularly and adequately monitor the Click2Gov systems and address vulnerabilities in the Click2Gov software by providing adequate patches to the municipalities or a failure to properly and timely install such patches.

24. In December 2018, Gemini Advisory covered the first wave of the Data Breach of CentralSquare's Click2Gov payment portal that affected dozens of cities across the United States and Canada between 2017 and late 2018.[6]

---

[5] *CEO Response to Reported Breach*, CENTRALSQUARE, FORMERLY SUPERION (Oct. 13, 2017), available at https://web.archive.org/web/20181202233703/www.superion.com/ceo-response-to-reported-breach/.

[6] *See* https://geminiadvisory.io/second-wave-of-click2gov-breaches-hits-united-states/.

25. In June 2018, CentralSquare released a statement in which it asserted it has addressed the issue with the Click2Gov payment portal system by deploying necessary patches to the impacted municipalities.

26. From August to October 2019, CentralSquare experienced the second wave of the Data Breach, which impacted the City of Norman and over thirty (30) other municipalities across the country.

27. Because of the ever-present and significant threat of Payment Data theft and the very serious risks associated with payment card data breaches, a need existed to ensure that the Click2Gov systems were adequately secured, including through necessary updates to security practices and protocols for the Click2Gov system.

28. CentralSquare, at all times relevant to this action, had duties to Plaintiffs and members of the Class to: (a) properly secure Payment Data submitted to or collected at municipality locations and on the impacted municipalities' internal networks; (b) encrypt Payment Data using industry standard methods; (c) use available technology to defend its systems from well-known methods of invasion; (d) act reasonably to prevent the foreseeable harms to Plaintiffs and the Class that may result from Payment Data theft; (e) promptly make available necessary Click2Gov software updates and patches to its municipality customers; and (f) promptly notify municipality customers and impacted citizens of any potential that citizens' Payment Data may have been compromised.

29. As a direct result of the Data Breach, many of the victims, including Plaintiffs and members of the Class, have suffered fraudulent charges, had their payment cards canceled, lost the use of their funds, lost time (i) contesting charges, (ii) trying to claw back

funds stolen from their bank accounts, and (iii) driving to and from banks and credit unions, and some have even had to cancel accounts.

30. Plaintiffs' and Class Members' also include the time-consuming requirements to (i) constantly scrutinize bank statements, (ii) obtain and pay for credit monitoring, (iii) check credit reports, (iv) contest false charges, and (v) engage in other efforts that require extensive amounts of time—and often out-of-pocket expenses.

31. Plaintiffs and Class Members are innocent Data Breach victims.

32. As a result of the Data Breach, Plaintiffs and Class Members suffered actual fraud and losses, including money being stolen from their bank accounts or from their credit accounts; loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of personal information; unreimbursed losses relating to fraudulent charges; losses and fees relating to exceeding credit and debit card limits, balances, and bounced transactions; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Payment Data.

B. Industry Standards and Governmental Guidance for Protection of Payment Data

33. Payment card processing companies have issued rules and standards governing the basic measures that merchants and payment software companies take to ensure that consumers' valuable Payment Data is protected.

34. The Payment Card Industry Data Security Standard ("PCI DSS") is a list of

twelve information security requirements that were promulgated by the Payment Card Industry Security Standards Council. The PCI DSS list applies to all organizations and environments where cardholder data is stored, processed, or transmitted, and requires companies to protect cardholder data, ensure the maintenance of vulnerability management programs, implement strong access control measures, regularly monitor and test networks, and ensure the maintenance of information security policies.

35. The twelve requirements of the PCI DSS are:

a. Install and maintain a firewall configuration to protect cardholder data;

b. Do not use vendor-supplied defaults for system passwords and other security parameters;

c. Protect stored cardholder data;

d. Encrypt transmission of cardholder data across open, public networks;

e. Protect all systems against malware and regularly update anti-virus software or programs;

f. Develop and maintain secure systems and applications;

g. Restrict access to cardholder data by business need to know;

h. Identify and authenticate access to system components;

i. Restrict physical access to cardholder data;

j. Track and monitor all access to network resources and cardholder data;

k. Regularly test security systems and processes; and

l. Maintain a policy that addresses information security for all personnel.[7]

36. Furthermore, PCI DSS sets forth detailed and comprehensive requirements that must be followed to meet each of the twelve mandates.

37. Payment software companies should be aware of their data protection obligations in light of their participation in the payment card processing networks.

38. Additionally, according to the Federal Trade Commission ("FTC"), the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act of 1914 ("FTC Act"), 15 U.S.C. § 45. *See, e.g., F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 245-47 (3d Cir. 2015); I*n re BJ's Wholesale Club, Inc.*, 140 F.T.C. 465 (2005).

39. As long ago as 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses use intrusion detection systems to expose a breach as soon as it occurs; monitor

[7]Payment Card International (PCI) Data Security Standard, "Requirements and Security Assessment Procedures, Version 3.2.1," (May 2018), https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1574069601944.

all incoming traffic for suspicious activity; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

40. The FTC has issued orders and received judgments against businesses that failed to employ reasonable measures to secure Payment Data. The FTC orders provide further notice and direction to businesses regarding their data security obligations. *See, e.g., Wyndham Worldwide Corp.*, 799 F.3d at 245-47; I*n re BJ's Wholesale Club, Inc.*, 140 F.T.C. 465.

C. The City of Norman Charged Fees for Security it Failed to Provide

41. Businesses are generally not allowed to charge extra fees or surcharges for credit or debit card payments. *See* 14A O.S. § 2-417. There is a limited exception, however, for municipalities. *See* 14A O.S. § 2-211(E).

42. This limited exception for municipalities caps the charge at the actual amount it costs to process the payment card transactions and provide secure payments.

43. Norman charged a $3.00 "convenience fee" for all debit or credit card transactions through the Click2Gov payment program. This fee is intended to assist Norman in paying to secure its online payment systems.

44. Because of subsection 2-211(E) and the nature of payment card transactions, the security of the transaction was a material part of the agreement between Plaintiff Doughty, members of the Norman Subclass, and Norman when they paid the $3.00 fee.

45. During the second wave of the Data Breach, which took place from August

to October 2019, Norman failed to provide this promised security.

46. In effect, therefore, during the time of the second wave of the Data Breach, Plaintiff and the Norman Subclass were paying an additional $3.00 fee for the convenience of giving identity thieves their Payment Data.

47. Every convenience fee collected by Norman for payment card transactions through Click2Gov during the months of August to October 2019 should be refunded to the Norman subclass.

D. Plaintiffs' Experiences with the Data Breach

Plaintiff Doughty

48. In August, September, and October 2019, Plaintiff Doughty used her debit card to pay her Norman utility bill online through the Click2Gov program.

49. Each time she used Click2Gov she was charged a $3.00 convenience fee by Norman.

50. On or around November 21, 2019, Plaintiff Doughty discovered that someone had stolen money from her checking account.

51. Between November 13 and 22, 2019, six (6) fraudulent transactions had been made using the debit card that she used to pay her Norman water bill on the Click2Gov software.

52. Altogether, a thief stole over $554.62 from her bank checking account.

53. As soon as she discovered the stolen funds, Plaintiff Doughty called her bank and reported the fraudulent transactions. She then called the vendors where the

fraudulent payments were made, including Chick-fil-A, Venmo, Lyft, and PayPal, to see if she could find out more information.

54. Plaintiff Doughty contested these transactions with her bank, which canceled her debit card, leaving her without access to her checking account for nearly two weeks. The bank eventually "provisionally" credited the stolen money back to her account while it investigated, but it warned her that it could claw back the money depending on the investigation. For over a month she was left not knowing whether the money would be clawed back or not, limiting her use of her money.

55. On December 10, 2019, Plaintiff Doughty received a letter from Norman notifying her that her debit card was compromised in the Data Breach. She promptly filed a police report with the Norman Police Department, notifying them of the fraudulent transactions that had occurred using the same debit card that she used to pay her Norman water bill.

56. Plaintiff Doughty spent over five (5) hours of her time responding to the Data Breach, including contesting the fraudulent charges, requesting a new debit card, filing a police report, and reviewing statements.

Plaintiff Fischer

57. Plaintiff Fischer used her debit card to pay her City of Margate utility bill online through CentralSquare's Click2Gov program.

58. On three separate occasions following the Data Breach, Plaintiff Fischer discovered that someone had stolen money from her checking account. Specifically,

between April 2017 and August 2017, three fraudulent transactions were made using the debit card that she used to pay her Margate water bill on the Click2Gov software. Altogether, a thief stole over $366.74 from her checking account.

59. Each time she discovered the stolen funds, Plaintiff Fischer was forced to call her bank and report the fraudulent transactions.

60. Plaintiff Fischer contested these transactions with her bank, which canceled her debit card each time she called in to report a new fraudulent transaction, leaving her without access to her checking account for days at a time. The bank eventually "provisionally" credited the stolen money back to her account while it investigated, but it warned her that it could claw back the money depending on the investigation, leaving her not knowing whether the money would be clawed back or not, which limited her use of her money.

61. It was in August 2017 that she became aware of the Data Breach through a City of Margate social media post, which informed the citizens of Margate of the Data Breach and resulting compromise of citizens' Payment Data.

62. Plaintiff Fischer subsequently filed a police report with the City of Margate Police Department, notifying them of the fraudulent transactions that had occurred using the same debit card that she used to pay her Margate water bill.

63. Plaintiff Fischer spent over six hours of her time responding to the Data Breach, including contesting the fraudulent charges, requesting new debit cards, filing a police report, and reviewing statements.

E. Plaintiffs and Class Members Suffered Damages

64. As alleged throughout this Complaint, Plaintiffs and Class Members have suffered injuries in fact that are traceable to the Data Breach.

65. The Payment Data of Plaintiffs and Class Members is private and sensitive in nature.

66. The Data Breach was a direct and proximate result of a failure to properly safeguard and protect Plaintiffs' and Class Members' Payment Data from unauthorized access, use, and disclosure.

67. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have experienced fraud and have been placed at an imminent, immediate, and increased risk of continued harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands in an effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports.

68. The theft and dissemination into the public domain of Plaintiffs' and Class Members' Payment Data has caused them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;

b. unauthorized charges on their debit and credit card accounts;

c. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their credit/debit card and personal information being placed in the hands of criminals and misused via the sale of Plaintiffs' and Class Members' information on the Internet's black market;

d. the improper disclosure of Plaintiffs' and Class Members' Payment Data;

e. loss of privacy;

f. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

g. ascertainable losses in the form of deprivation of the value of their Payment Data, for which there is a well-established national and international market;

h. loss of use of, and access to, their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and

i. the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection

services, imposition of withdrawal and purchase limits on compromised accounts, and the inconvenience, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

69. Plaintiffs and Class Members have an undeniable interest in ensuring that their Payment Data is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

CLASS ALLEGATIONS

70. Plaintiffs incorporate by reference the preceding paragraphs as if fully set forth herein.

71. Plaintiffs, pursuant to Fed. R. Civ. P. Rule 23(a), (b)(2), (b)(3), and (c)(4), bring all claims as Class claims and seek relief on behalf of themselves and as a representative of all others who are similarly situated, asserting claims on behalf of the following classes (collectively the "Class Members" or the "Class"):

Nationwide Class against CentralSquare (the "Nationwide Class"):

> All residents of the United States whose Payment Data was used to pay utility bills and/or other payments through CentralSquare's Click2Gov payment portal between January 1, 2017, and December 31, 2019.

City of Norman, Oklahoma subclass (the "Norman Subclass"):

> All persons who were charged convenience fees for payment card transactions on the Click2Gov payment portal at the City of Norman, Oklahoma between August and October 2019.

72. Excluded from the Class are CentralSquare and any entity in which CentralSquare has a controlling interest, as well as CentralSquare's officers, directors, legal

representatives, successors, subsidiaries, and assigns. The Class also excludes any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

73. Plaintiffs reserve the right to amend the above class definitions or to seek additional subclasses as necessary.

A. Class Certification is Appropriate

74. The proposed Nationwide Class and Norman Subclass meet the requirements of Rule 23(a), (b)(2), (b)(3), and (c)(4) as required.

75. *Numerosity*: The proposed Classes are so numerous that joinder of all members is impracticable. While the total number of individuals affected by the Data Breach is unknown, based on reporting, the Norman Subclass may include several thousand city utilities customers. The Nationwide Class is much larger, including hundreds of thousands of residents of what appears to be "46 confirmed impacted local governments."[8] *See* Fed. R. Civ. P. 23(a)(1).

76. *Commonality and Predominance*: Common questions of law and fact exist as to Plaintiffs and all members of the proposed Classes. These questions predominate over the questions affecting individual Class Members. These common legal and factual questions include, but are not limited to, the following:

As to the Nationwide Class and CentralSquare:

a. Whether CentralSquare engaged in the wrongful conduct alleged herein;

[8] *See* https://threatpost.com/patched-click2gov-flaw-still-afflicting-local-govs/140109/.

b. Whether CentralSquare owed a duty to Plaintiffs and Class Members to adequately protect their Payment Data, and whether it breached this duty;

c. Whether CentralSquare breached federal and state laws, thereby breaching its duties to Plaintiffs and the Class as a result of the Data Breach;

d. Whether CentralSquare's contract with the impacted municipalities (and the representations therein) created third-party beneficiary contracts;

e. Whether CentralSquare breached third-party beneficiary contracts by failing to protect Plaintiffs' and Class Members' Payment Data;

f. Whether Defendant breached implied contracts with Plaintiffs and Class Members by failing to protect their Payment Data;

g. Whether CentralSquare knew or should have known that its Click2Gov payment portal was vulnerable to attacks from hackers and cyber criminals;

h. Whether CentralSquare's conduct, including any failure to act, resulted in the breach of its computer and network systems resulting in the theft of customers' Payment Data;

i. Whether Plaintiffs and members of the Class suffered injury as a proximate result of CentralSquare's conduct or failure to act; and

j. Whether Plaintiffs and the Class are entitled to recover compensatory damages, equitable relief, and other relief, and the extent of the remedies that should be afforded to Plaintiffs and the Class;

As to the Norman Subclass and the City of Norman:

a. Whether Norman made representations to Plaintiff Doughty and Norman Subclass Members regarding the privacy and security of their payment cards if used on its website;

b. Whether Norman's representations created implied contracts;

c. Whether Norman sufficiently addressed, remedied, or protected Plaintiff Doughty and Norman Subclass Members following the Data Breach and took adequate preventative and precautionary measures to ensure Plaintiff Doughty and the Norman Subclass Members will not experience further harm;

d. Whether Plaintiff Doughty and members of the Norman Subclass had contracts with Norman that included secure transactions, and whether Norman breached those contracts;

e. Whether Norman received money from Plaintiff Doughty and members of the Norman Subclass to provide for secure transactions;

f. Whether Plaintiff Doughty and members of the Norman Subclass failed to receive from Norman the security they paid for;

g. Whether it would be unjust for Norman to retain money received from Plaintiff Doughty and members of the Norman Subclass;

h. Whether Plaintiff Doughty and members of the Norman Subclass are entitled to reimbursement for money Norman received from them; and

i. Whether Plaintiff Doughty and Norman Subclass Members are entitled to recover damages, equitable relief, and other relief, and the extent of the remedies that should be afforded to Plaintiff Doughty and the Norman Subclass.

77. These questions are common to all Class Members' claims and predominate over any and all individual claims that might exist. *See* Fed. R. Civ. P. 23(a)(2) and (b)(3).

78. *Typicality*: Plaintiffs' claims are typical of the claims of the Class Members. Plaintiffs and members of the Class were injured through CentralSquare's and, to the extent applicable, Norman's, uniform misconduct. The same Click2Gov payment software and the same event and conduct that gave rise to Plaintiffs' claims are identical to those that give rise to the claims of every other member of the Class because Plaintiffs and Class Members had their sensitive Payment Data compromised in the same way by the same conduct. *See* Fed. R. Civ. P. 23(a)(3).

79. *Adequacy*: Plaintiffs are adequate representatives of the Class because Plaintiffs' interests do not conflict with the interests of the Class that they seek to represent; Plaintiffs have retained counsel competent and highly experienced in complex litigation (and particularly data breach class action litigation); Plaintiffs and Plaintiffs' counsel intend to prosecute this action vigorously; and the interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel. *See* Fed. R. Civ. P. 23(a)(4).

80. *Superiority*: A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class. The injury suffered by each

individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be difficult, if not impossible, for members of the Class to redress Defendants' wrongdoing individually and effectively. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. *See* Fed. R. Civ. P. 23(b)(3).

81. *Injunctive and Declaratory Relief*: Class certification is also appropriate under Rule 23(b)(2) and (c). Defendant CentralSquare, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

82. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether CentralSquare failed to timely notify Plaintiffs and Class Members of the Data Breach;

b. Whether CentralSquare owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Payment Data;

c. Whether CentralSquare's security measures to protect its Click2Gov payment portal system were reasonable in light of the PCI DSS requirements, FTC data security recommendations, and other best practices recommended by data security experts;

d. Whether CentralSquare failed to take commercially reasonable steps to safeguard the Payment Data of Plaintiffs and Class Members; and

e. Whether adherence to PCI DSS requirements, FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

83. Finally, all members of the proposed Class are readily ascertainable. CentralSquare has access to information regarding which of the cities were impacted by the Data Breach. Norman also maintains the information of the impacted citizens on its systems. Using this information, Class Members can be identified, and their contact information ascertained, for the purpose of providing notice to the Class.

CAUSES OF ACTION

COUNT I - NEGLIGENCE

84. Plaintiffs reallege and incorporate the preceding paragraphs as though fully set forth herein.

85. CentralSquare's Click2Gov payment portal collected Payment Data from Plaintiffs and Class Members in exchange for public utilities payments and other services made available online to Plaintiffs.

86. Upon accepting and storing the Payment Data of Plaintiffs and Class Members in its Click2Gov payment portal, CentralSquare undertook and owed a duty to Plaintiffs and Class Members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. CentralSquare knew that Payment Data was private and confidential and should be protected as private and confidential.

87. CentralSquare owed a duty of care not to subject Plaintiffs and Class Members, along with their Payment Data, to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate data security practices.

88. CentralSquare owed a duty to Plaintiffs and the Class to maintain confidentiality and to exercise reasonable care in safeguarding and protecting their financial and personal information on the Click2Gov payment portal from being compromised by unauthorized persons. This duty included, among other things, designing, maintaining, and testing CentralSquare's Click2Gov payment portal to ensure that Plaintiffs' and Class Members' financial and personal information on the Click2Gov payment portal was adequately protected in the process of collection and following collection while stored on the Click2Gov payment portal.

89. CentralSquare owed a duty to Plaintiffs and Class Members to implement processes that would detect a breach of the Click2Gov payment portal in a timely manner and to timely act upon warnings and alerts, including those generated by its customers and own security systems.

90. CentralSquare owed a duty to Plaintiffs and Class Members to provide security consistent with industry standards and requirements and to ensure that its Click2Gov payment portal—and the personnel responsible for them—adequately protected the financial and personal information of Plaintiffs and Class Members whose confidential data was obtained and maintained on the Click2Gov payment portal.

91. CentralSquare knew, or should have known, the risks inherent in collecting and storing the financial and personal information of Plaintiffs and Class Members and of the critical importance of providing adequate security for that information.

92. CentralSquare knew, or should have known, that its Click2Gov payment portal did not adequately safeguard Plaintiffs' and Class Members' Payment Data.

93. CentralSquare's negligent conduct created a foreseeable risk of harm to Plaintiffs and Class Members. This conduct included, but was not limited to, CentralSquare's failure to take the steps and opportunities to prevent and/or detect and mitigate the impact of the Data Breach.

94. CentralSquare breached its duty to Plaintiffs and Class Members to adequately protect and safeguard their Payment Data by disregarding standard information security principles and protocols, and by allowing unmonitored and unrestricted access to unsecured Payment Data. CentralSquare failed to provide adequate supervision and oversight of the Payment Data with which they were and are entrusted, which permitted an unknown third party to gather the Payment Data, misuse the Payment Data, and intentionally disclose it to others without consent.

95. CentralSquare breached its duties to Plaintiffs and Class Members by failing to provide a fair, reasonable, or adequate Click2Gov payment portal to safeguard Plaintiffs' and Class Members' Payment Data.

96. Because CentralSquare knew that a breach of its Click2Gov payment portal would damage hundreds of thousands of citizen customers, including Plaintiffs and Class Members, CentralSquare had a duty to adequately protect its Click2Gov payment portal and the Payment Data contained thereon.

97. Plaintiffs' and Class Members' willingness to entrust CentralSquare with their Payment Data was predicated on the understanding that CentralSquare would take adequate security precautions to safeguard that information.

98. CentralSquare also had independent duties under state and federal laws requiring it to reasonably safeguard Plaintiffs' and Class Members' Payment Data and promptly notify them about the Data Breach.

99. CentralSquare breached its duties to Plaintiffs and Class Members in numerous ways, including:

a. by failing to provide a fair, reasonable, or adequate Click2Gov payment portal to safeguard Plaintiffs' and Class Members' Payment Data;

b. by creating a foreseeable risk of harm through the misconduct previously described;

c. by failing to implement adequate security systems, protocols, and practices sufficient to protect Plaintiffs' and Class Members' Payment

Data; and

d. by failing to comply with industry standard data security standards during the period of the Data Breach.

100. Through CentralSquare's acts and omissions described in this Complaint, including CentralSquare's failure to provide adequate security and its failure to protect Payment Data of Plaintiffs and Class Members from being foreseeably captured, accessed, disseminated, stolen and misused, CentralSquare unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiffs' and Class Members' Payment Data while it was within the Click2Gov payment portal.

101. Upon information and belief, CentralSquare improperly and inadequately safeguarded Plaintiffs' and Class Members' Payment Data in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. CentralSquare's failure to take proper security measures to protect sensitive Payment Data created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of Plaintiffs' and Class Members' Payment Data.

102. CentralSquare's conduct was negligent and departed from reasonable standards of care, including, but not limited to, failing to adequately protect the Payment Data; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to the Click2Gov system and Payment Data of Plaintiffs and Class Members; and failing to provide a safe Click2Gov product to its municipality customers and/or all necessary Click2Gov software updates and patches to its municipality customers.

103. Neither Plaintiffs nor the other Class Members contributed to the Data Breach and subsequent misuse of their Payment Data, as described in this Complaint.

104. As a direct and proximate cause of CentralSquare's conduct, Plaintiffs and the Class suffered damages, including but not limited to, damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of their Payment Data; damages arising from Plaintiffs' and Class Members' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports, and damages from identity theft.

105. As a direct and proximate result of CentralSquare's negligent conduct, Plaintiffs and Class Members have been injured and are entitled to actual damages in amounts to be proven at trial.

COUNT II – BREACH OF IMPLIED CONTRACT

106. Plaintiffs reallege and incorporate the preceding paragraphs as though fully set forth herein.

107. CentralSquare invited Plaintiffs and Class Members to utilize its Click2Gov payment portal to make their utilities bill payments online. Plaintiffs and Class Members

accepted CentralSquare's offer and used their credit or debit cards to pay for their utilities bills through the Click2Gov online payment portal webpage, which was accessible through municipality websites.

108. When Plaintiffs and Class Members utilized CentralSquare's services, they provided their Payment Data, including but not limited to the personally identifiable information ("PII") and Payment Data contained on the face and embedded in the magnetic strip of their debit and credit cards. By so doing, Plaintiffs and Class Members entered into mutually agreed upon implied contracts with CentralSquare, pursuant to which Plaintiffs and Class Members agreed that their payment cards were valid and would provide compensation for their purchases, while CentralSquare agreed that it would use the Payment Data of Plaintiffs and Class Members in its possession for only the agreed-upon payment and no other purpose.

109. Implicit in the agreement by CentralSquare to use the Payment Data in its possession for only the agreed-upon payment and no other purpose was the obligation that CentralSquare would use reasonable measures to safeguard and protect the Payment Data of Plaintiffs and Class Members in the Click2Gov payment portal.

110. By accepting the payment cards on its Click2Gov payment portal, CentralSquare assented to and confirmed its agreement to reasonably safeguard and protect the Payment Data of Plaintiffs and Class Members from unauthorized disclosure or uses.

111. Plaintiffs and Class Members would not have provided and entrusted their Payment Data, including all information contained in the magnetic strips of their credit and

debit cards, to CentralSquare in the absence of the implied contracts they made with CentralSquare.

112. Plaintiffs and Class Members fully performed their obligations under the implied contracts.

113. CentralSquare breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect the PII and Payment Data of Plaintiffs and Class Members.

114. CentralSquare breached the implied contracts it made with Plaintiffs and Class Members by failing to ensure that the Payment Data of Plaintiffs and Class Members in its possession was used only for the agreed-upon utilities bill payment and no other purpose.

115. Plaintiffs and Class Members utilized services from CentralSquare and provided CentralSquare with their payment information. In exchange, Plaintiffs and Class Members should have been entitled to have CentralSquare protect their Payment Data with adequate data security.

116. CentralSquare knew that Plaintiffs and Class Members conferred a benefit on CentralSquare through their use of the Click2Gov payment portal, and CentralSquare accepted or retained that benefit. CentralSquare profited from Plaintiffs' and Class Members' use of the Click2Gov payment portal.

117. CentralSquare failed to secure the Payment Data of Plaintiffs and Class Members and, therefore, did not provide full consideration for the benefit the Plaintiffs and Class Members provided.

118. CentralSquare's Click2Gov payment portal acquired the Payment Data through inequitable means and CentralSquare failed to disclose the inadequate security practices previously alleged.

119. If Plaintiffs and Class Members had known that CentralSquare would employ inadequate security measures to safeguard their Payment Data, they would not have made the bill payments online.

120. As a direct and proximate result of CentralSquare's breaches of the implied contracts between CentralSquare and Plaintiffs and Class Members, Plaintiffs and the Class sustained actual losses and damages as described in detail above.

121. Plaintiffs and Class Members were harmed as the result of CentralSquare's breach of the implied contracts because their Payment Data was compromised and disclosed to third parties without their consent, placing them at a greater risk of, and subjecting them to, identity theft. Plaintiffs and the Class have also suffered consequential out-of-pocket losses for procuring credit freeze or protection services, identity theft monitoring, late fees, bank fees, and/or other expenses relating to identity theft losses or protective measures. The Class is further damaged as their Payment Data remains in the hands of those who obtained it without their consent.

122. This breach of implied contracts was a direct and legal cause of the injuries and damages to Plaintiffs and Class Members as described above.

COUNT III – BREACH OF CONTRACT
(Against the City of Norman, on behalf of the Norman Subclass)

123. Plaintiffs reallege and incorporate the preceding paragraphs as though fully set forth herein.

124. Plaintiff Doughty and Norman Subclass Members conferred a monetary benefit upon Norman in the form of monies paid for the purchase of goods and services from the municipality.

125. Norman appreciated or had knowledge of the benefits conferred upon it by Plaintiff Doughty and Norman Subclass members. Norman also benefited from receipt of Plaintiff Doughty's and Norman Subclass members' Payment Data, as such was utilized by Norman to facilitate payment to it.

126. The convenience fees that Plaintiff Doughty and the Norman Subclass paid to Norman were supposed to be used by Norman to pay for the administrative costs of reasonable data privacy and security practices and procedures.

127. Under principals of equity and good conscience, Norman should not be permitted to retain the money belonging to Plaintiff Doughty and Norman Subclass because Norman failed to provide the promised security and was in effect charging them money to expose them to identity theft.

128. Norman should be compelled to refund the fees it charged Plaintiff Doughty and the Norman Subclass for the use and safety of their electronic payment systems, along with the costs and attorney fees incurred in recovering these fees.

COUNT IV – UNJUST ENRICHMENT
(Against the City of Norman, on behalf of the Norman Subclass)

129. Plaintiffs reallege and incorporate the preceding paragraphs as though fully set forth herein.

130. This claim is pled in the alternative to the above breach of contract claim.

131. Plaintiff Doughty and Norman Subclass Members conferred a monetary benefit upon Norman in the form of monies paid for the purchase of goods and services from the municipality.

132. Norman appreciated or had knowledge of the benefits conferred upon it by Plaintiff Doughty and Norman Subclass members. Norman also benefited from receipt of Plaintiff Doughty's and Norman Subclass members' Payment Data, as such was utilized by Norman to facilitate payment to it.

133. The convenience fees that Plaintiff Doughty and the Norman Subclass paid to Norman were supposed to be used by Norman to pay for the administrative costs of reasonable data privacy and security practices and procedures.

134. Under principals of equity and good conscience, Norman should not be permitted to retain the money belonging to Plaintiff Doughty and the Norman Subclass because Norman failed to provide the promised security and was in effect charging them money to expose them to identity theft.

135. Norman should be compelled to refund the fees it charged Plaintiff Doughty and the Norman Subclass for the use and safety of their electronic payment systems, along with the costs and attorney fees incurred in recovering these fees.

COUNT V – DECLARATORY RELIEF
(On behalf of the Nationwide Class)

136. Plaintiffs reallege and incorporate the preceding paragraphs as though fully set forth herein.

137. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief.

138. An actual controversy has arisen in the wake of the Data Breach regarding CentralSquare's common law and other duties to reasonably safeguard its citizen users' Payment Data.

139. The Court should also issue prospective injunctive relief requiring CentralSquare to employ adequate security practices consistent with law and industry standards to protect consumers' Payment Data.

140. The replacement of a payment card compromised in the Data Breach does not alleviate the harm that may come to Plaintiffs and Class Members as their Payment Data remains on CentralSquare's Click2Gov payment portal and as they must continue to make their bill payments through the Click2Gov payment portal.

141. Furthermore, even though a payment card may be expired or replaced, a hacker or scammer may be able to use an expired or replaced payment card account stolen in a data breach to conduct transactions long after the breach. Further, if a hacker or scammer has used a stolen payment card to open a merchant account using the cardholder's name, the card information in the fraudulent account may be updated automatically when the card is reissued after a data breach, given agreements between some merchants and payment card processors.

142. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury, and lack an adequate legal remedy in the event of another data breach at CentralSquare's Click2Gov payment portal. The risk of another such breach is real, immediate, and substantial.

143. The hardship to Plaintiffs and Class Members if an injunction does not issue exceeds the hardship to CentralSquare if an injunction is issued. Among other things, if another data breach occurs at CentralSquare's Click2Gov payment portal, Plaintiffs and Class Members will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to CentralSquare of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and CentralSquare has a pre-existing legal obligation to employ such measures.

144. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by helping to prevent another data breach at CentralSquare's Click2Gov payment portal, thus eliminating the additional injuries that would result to Plaintiffs and other consumers whose Payment Data would be further compromised.

145. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that CentralSquare must implement and maintain reasonable security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits on CentralSquare's Click2Gov

payment portal on a periodic basis, and ordering CentralSquare to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. purging, deleting, and destroying Payment Data not necessary for its provisions of services in a reasonably secure manner;

e. conducting regular database scans and security checks;

f. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

g. educating its municipality customers about the threats they face as users of the Click2Gov payment platform, and of the potential for loss of their citizens' financial and personal information to third parties, as well as the steps CentralSquare users (both municipalities and citizen users) should take to protect themselves.

PRAYER FOR RELIEF

Plaintiff Doughty and Plaintiff Fischer, on behalf of themselves and all others similarly situated, respectfully requests that the Court grant the following relief:

a. Certifies a nationwide class against CentralSquare and a subclass of affected residents in the City of Norman, Oklahoma;

b. Award Plaintiffs and the Class appropriate monetary relief, including actual damages, restitution, and disgorgement.

c. Award damages to the Norman Subclass for all convenience fees charged from August to October 2019, which is a refund of the monthly $3.00 fees that each member of the Norman Subclass paid to the City of Norman from August to October 2019;

d. Award Plaintiffs and the Class equitable, injunctive and declaratory relief as may be appropriate, including (i) appropriate injunctive relief designed to protect against the recurrence of a data breach through the adoption and implementation of best security data practices to safeguard municipality and citizen customers' financial and personal information, and (ii) an extension of credit monitoring services and similar services to protect against all types of identity theft, especially including card theft and fraudulent card charges;

e. Enter an order requiring Defendants to pay the necessary costs involved in notifying the Class Members about the judgment and administering the claims process;

f. Enter judgment in favor of Plaintiffs and the Class awarding them pre-judgment and post-judgment interest, reasonable attorney fees, costs and expenses as allowably by law; and

g. Any other favorable relief as allowable under law or at equity.

Dated: January 26, 2022

Respectfully Submitted,

/s/ William B. Federman
William B. Federman, OBA # 2853
Molly E. Brantley, OBA #33126
FEDERMAN & SHERWOOD
10205 N. Pennsylvania
Oklahoma City, OK 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
wbf@federmanlaw.com
meb@federmanlaw.com

Attorneys for Plaintiffs and the Putative Class

CERTIFICATE OF SERVICE

I hereby certify that on January 26, 2022 I electronically filed the foregoing document with the Clerk of the Court using CM/ECF. I also certify that the foregoing document is being served this day on all counsel of record via transmission of Notices of Electronic filing generated by CM/ECF or in some other authorized manner for those counsel or parties who are not authorized to receive electronically Notices of Electronic Filing.

By: */s/ William B. Federman*